REMARKS

Applicant acknowledges that the previous rejection under 35 USC 112 has been withdrawn.

Claim 31 has been amended to overcome the objection thereto and the rejection of claim 31 should now also be withdrawn.

The rejection of claims 36-38 under 35 USC 102(b) as being anticipated by US Patent 6,405,369 to Tsuria is respectfully traversed.

Applicant has further amended claim 36 to make it clear that the removable security interface of the subject invention is designed for pairing one unique digital data reception equipment with a plurality of access control cards of one or more external security modules to manage access to digital data distributed by an operator with each access control card having a unique identifier and containing information about access rights of a subscriber to said digital data.

The removable security interface further comprises means for recording the identifier of each access control card in the non-volatile memory and at least one data processing algorithm for use by the decoder in the reception equipment to activate or deactivate the pairing of the reception equipment to the access control cards.

Claim 36 is not anticipated by Tsuria since Tsuria does not teach a removable security interface for activating a matching function between one decoder

represented by a unique reception equipment for pairing this decoder with a plurality of different external security modules. The second smart card taught in Tsuria is used for activating the decoding of pay television transmission in a second decoder when the pay television transmission is not already decoded by a first smart card in a first decoder. Accordingly, the second smart card in Tsuria is not an interface between the decoder of one digital data reception equipment and a plurality of access control cards of one or more external security modules containing information about access rights of a subscriber to the digital data. Moreover, Tsuria requires "chaining data" inclusive of either a signature, a key, or a seed to correlate and validate, identify and authenticate the second smart card. This is an entirely different methodology from that taught in the subject application and in which no such "chaining data" is required. For a rejection to be valid under 35 USC 102, the reference must teach each and every element in the claim which is not the case in Tsuria since the second smart card in Tsuria must possess chaining data linking it to the first smart card for pairing and cannot pair the reception equipment of one decoder to a plurality of access cards of one or more external security modules without such "chaining data". Moreover, the second smart card does not contain means for recording the identifier of each access control card in the non-volatile memory and does not contain an algorithm for use by the one decoder to activate or deactivate the pairing of the one decoder to the control cards. Since Tsuria uses two (2) decoders, not one, it is <u>not</u> pairing one decoder to access cards as is claimed in amended claim 36.

Accordingly, the rejection of claim 36 under 35 USC 102 should be withdrawn.

The rejection of claims 1, 5-8, 10-18, 24-35 and 39-47 under 35 USC 103(a) as being unpatentable over Tsuria in view of USP 7,457,967 to Cocchi et al is respectfully traversed.

Applicant believes the Examiner has misinterpreted Col. 7, lines 44-53 of Tsuria which reads as follows:

"The chaining data may include a signature, a key or a seed which may be employed to at least one of validate, identify, verify and authenticate the second smart card. Preferably the chaining data also includes a digital representation of a time increment which may be employed to calculate a deactivation data. The time increment is typically specified in months and days."

Note that in lines 51-53 Tsuria uses the signature for checking authentication for validity in the decoder processor which forms part of the first decoder, such as decoder processor 26 of Fig. 1. Accordingly, it appears that chaining data in Tsuria is essential to activate the second smart card and to verify whether or not said second smart card can be used for decoding the pay television programs using the second decoder.

In contrast, the method of the subject invention as claimed controls the pairing of one digital data reception equipment with one or more different external security modules belonging to different users in order to allow said different users to

decode the digital data by means of the unique decoder. Stated otherwise, the computer in the subject invention determines whether or not an external security module just connected to the unique digital data reception equipment is already memorized from an updated list transmitted to the reception equipment and comprising only external security modules identifiers matched to the unique digital data reception equipment.

Tsuria does not involve the pairing of a unique digital data reception equipment with a plurality of different external security modules, but instead involves the use of at least two decoders for decoding the same program, using a first smart card with the first decoder, and a second smart card with the second decoder. To accomplish this, the first and second smart cards in Tsuria must be linked by means of chaining data which needs to be verified.

Claim 1 of the subject invention involves the pairing of one unique digital data reception equipment with one or more different external security modules. Tsuria requires the existence of "chaining data" such as a signature key or seed which is used to validate, identify or authenticate the second smart card. This link between the first and second smart cards in Tsuria does not exist in the method of claim 1. In Tsuria, the verification of this link of "chaining data" is essential to determine whether the first smart card or the second is to be used.

Moreover, as set forth in claims 1 and 36, as amended, the method is limited to the pairing of one unique digital data reception equipment to one or more different external security modules each having a unique identifier and with each of the

different security modules being adapted to cooperate with said one digital data reception equipment. Stated otherwise, applicants method involves the use of only one decoder to be paired with one or more external security modules. This is not taught or suggested in Tsuria which does not involve the pairing of the digital data reception equipment to one or more of different external security modules but instead involves the use of two decoders for decoding the same program using either a first smart card with the first decoder and/or a second smart card with the second decoder. This is an entirely different method of operation and uses an entirely different apparatus from that disclosed and claimed in the present invention.

Moreover, contrary to the allegation of the Examiner, Tsuria is not involved in verifying whether or not the identifier of an external security module just connected to a digital data reception equipment is already memorized from an updated list of external security module identifiers transmitted to the reception equipment and therefore, it makes no sense for combining Tsuria with Cocchi et al as suggested by the Examiner. Tsuria involves two decoders to decode a program for determining which of the two smart cards to choose from.

For all of the above reasons, the rejection of claims 1, 5-8, 10-18, 24-35, 39-47, should be withdrawn.

Reconsideration and allowance of claims 1, 5-8, 10-18, 24-47, is respectfully solicited.

Respectfully submitted,

Dated: September 7, 2010
(September 6, 2010, Labor Day Holiday)

Eugene Lieberstein
Registration No. 24,645

Customer # 79681
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
Tel: 212-589-4634
Fax: 212-589-4201

CERTIFICATE OF MAILING

I hereby certify that this Amendment is being submitted to the USPTO via First Class Mail, addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria VA 22313-1450, on September 7, 2010.

By_____